

REMARKS

Claim 1 is pending in the present application. In response to the Office Action mailed May 12, 2004, applicants submit the following remarks.

In paragraph 2, the Office Action has rejected claim 1 for allegedly being unpatentable under 35 USC 103(a) over US Patent No. 5,903,882 issued to Alan Asay et al. (“Asay”). The Office Action has summarized many alleged features of Asay without comparing them to particular limitations of the claimed invention in providing the basis for the rejection. The Office Action also does not allege that Asay anticipates the claimed invention— thus, conceding that Asay does not teach each and every limitation of the claimed invention.

Applicants respectfully traverse the allegation that the claimed invention is unpatentable in view of Asay. As an initial matter, Asay does not teach, disclose, or suggest all of the limitations of the claimed invention. Moreover, these limitations are not obvious from Asay’s disclosure. Examples of such limitations include (i) the warranty comprising a contract between the entity and the subscriber, a relying party being a third-party beneficiary to the contract; (ii) receiving a request for a warranty from the subscriber to whom the entity issued a digital certificate; and (iii) receiving a validation request from the relying party. These limitations spell out details demonstrating that the claimed invention is significantly different from Asay.

The claimed invention provides a solution, of particular utility in the context of the four-corner model, to the problem of providing warranties for facts associated with a digitally-signed electronic message. The claimed invention provides the warranties while preserving the four-corner model’s efficient protection of confidential information and privacy. Structuring electronic transactions using the four-corner model is advantageous in that it readily leverages the existing knowledge of financial institutions and entities in promoting reliable transactions entered into by their customers. This extension of the familiar experience of the customers in using their respective financial institutions results in lower costs and increased reliability.

In the four-corner model a subscriber and a relying party are not required to directly verify each other’s credentials. Instead, the subscriber uses its own issuing financial institution as its certificate authority while the relying party uses its relying

financial institution as its certificate authority, thus defining the four corners. The issuing and relying financial institutions typically interact with each other in the context of many transactions. This knowledge is then also reflected in their mutual authentication by a commonly accepted root certificate authority. Thus, the information required for mutual authentication via the financial institutions is different than that required by either the subscribing customer or relying customer in direct interactions.

As a result, less confidential information is required for successful authentication in the four-corner model. As an example, unlike Asay's teaching that the certificate authority sends the primary certificate to the reliance server, see, e.g., column 5, lines 2-6 of Asay in the 'Summary of the Invention,' there is no such requirement in the four-corner model. Moreover, instead of the relying party contracting with the reliance server, in accordance with the claimed invention the relying party seeks validation of the warranty contract between the subscriber and the issuing participant. Validation typically establishes that the relying party is the third-party beneficiary of the contract between the subscriber and the issuing participant.

In part, as a result of the above considerations the four-corner model enhances privacy and makes transactions reliable and fast. Notably, vouching by the financial institutions for their clients' provides indirection in the four-corner model to preserves confidential client information. As is apparent, the four-corner model's information flow not only reduces the overhead compared to Asay's disclosure, but provides a method that is readily scalable.

However, in accordance with Asay, in the four-corner model a relying customer would directly contract with the issuing participant rather than use its own bank, the relying participant. This is in agreement with Asay's teaching that it is undesirable for the relying party to be a third party beneficiary. As a result, this feature further distinguishes the claimed invention from Asay. Indeed, Asay discloses several steps taken to avoid the relying party being a third party beneficiary. For instance, while the claimed invention recites that it is the subscribing customer who requests, directly or indirectly, the warranty, Asay teaches that the relying party requests the warranty. See column 5, lines 7-17 of Asay.

The cumbersome strategies disclosed by Asay may also require extensive disclosure of otherwise sensitive confidential information. For instance, Asay discloses a potentially risky confluence of information at the reliance server. This confluence is easily seen in Figure 3 of Asay. Figure 3 shows the Reliance Server 104 receiving extensive information from the Certification Authority 102, the Relying Party 108, and Other Party 1240. This makes the reliance server a natural candidate for security breaches. Moreover, the resulting increased message load at the reliance server makes Asay's disclosed system not as scalable as the claimed invention.

In other words, Asay discloses making warranties by assembling far more information than that required by the claimed invention. Thus, Asay's teachings increase the risk of privacy violations. In addition, the system of Asay is not as simple and scalable for automated operations as the claimed invention.

Turning to the specific limitations, the claimed invention includes the limitation "the warranty comprising a contract between the entity and the subscriber, a relying party being a third-party beneficiary to the contract." In sharp contrast, as discussed above, Asay requires the relying party to request the warranty and be party to the contract with the reliance server. See, for instance, Figure 3 and column 5, lines 7-17 of Asay. Thus, Asay also does not teach the limitation "receiving a request for a warranty from a subscriber to whom the entity issued a digital certificate" of the claimed invention. Accordingly, the warranty request made by the subscriber – not the relying party – further serves to distinguish the claimed invention from Asay.

Indeed, Asay teaches away from the claimed invention because it views warranties as being acquired and properly paid for by the relying party. According to Asay, "the subscriber forms a transaction and then provides the transaction to a relying party," which party may elect to request assurances about the "the primary certificate issued by the certification authority" from a reliance server. See column 5, lines 7-17 of Asay. The reliance server, in the event it approves the request, issues a secondary certificate with the requested warranty to the relying customer.

Figures 3 and 5 of Asay show the details for the relying party being responsible for requesting and paying for the warranty. Figure 3 shows the relying party 108 directly requesting, via request 116, a secondary certificate from reliance server 104.

Figure 5 shows the payment details for the 'reliance check' in request 116. This aspect of Asay is also explained in the text, e.g., column 5, lines 11-18, and columns 18-19.

In accordance with the claimed invention, the relying party may request validation of the digital certificate of the issuing financial institution. Plainly this validation request is not the same as Asay's warranty request. A successful validation request may advantageously identify the third party beneficiary of the contract between the issuing financial institution and the subscribing customer without ambiguity, but it does not constitute the warranty request itself.

It is also apparent that in the method of the invention, fewer exchanges of sensitive information are required than in methods disclosed by Asay. For instance, all certificates are not automatically sent to a single reliance server. This both reduces the overhead and improves scalability.

Therefore, the rejection of claim 1 as being obvious in view of Asay should be withdrawn. In sharp contrast to Asay, the simplified yet secure method provided by the claimed invention preserves privacy and leverages the longstanding relations between financial institutions and their clients and between financial institutions. Thus, with the help of the invention, financial institutions can use their knowledge and manage their exposure to risk while better using their resources and their respective customer base. The privacy of customers is preserved throughout a transaction since there is no single entity like a reliance server of Asay that is routinely entrusted with information about the subscriber, the certificate authority, the relying party and assurance limits. At the same time the system is efficient and readily scalable for even global operations.

CONCLUSION

All of the rejections made by the Office Action have been addressed and overcome. Therefore, the pending claim 1 is allowable. Accordingly, it is respectfully requested that the present application be allowed to proceed to issuance without delay.

The original due date for this Response was August 12, 2004. Accordingly, a Petition for Extension of Time (one month) is filed herewith, which renders this Response timely today since September 12, 2004 was a Sunday. Please charge any required fees in connection with this Response to JONES DAY Deposit Account No. 50-3013.

In light of the above, it is respectfully submitted that the present application is in condition for allowance. Favorable disposition is respectfully requested.

Date September 13, 2004

Respectfully submitted,



Rattan Nath (Reg. No. 43,827)

for

Rory J. Radding (Reg. No. 28,749)

JONES DAY
222 East 41st Street
New York, New York 10017
(212) 326-3939